IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH KIDCASH@HOTMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION, USA	Case No. 1:24-mj- 02-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Patrick Latchaw, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Microsoft, an email provider headquartered at 1 Microsoft Way, Redmond, Washington 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Treasury Inspector General for Tax Administration ("TIGTA"), assigned to the Northeast Field Division, Boston Field Office, Boston, Massachusetts. I have been a TIGTA Special Agent since January 2021. Prior to employment with TIGTA, I was employed as a Special Agent with the Department of State, Bureau of Diplomatic Security Service ("DSS"). In preparation for this assignment, and as part of my

continued education, I have successfully completed law enforcement and financial crimes focused training, including formal courses and training exercises. I have participated in many aspects of federal investigations including, but not limited to: subject, victim, and witness interviews; analysis of telephone, email, and financial records; and assisting with the preparation and execution of arrest and/or search warrants. As a federal agent, I am authorized to investigate violations of the laws of the United States. As a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. § 1014 (False Statement to a Bank) (collectively the "Subject Offenses") have been committed by Sully Pimentel. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. In response to the coronavirus (COVID-19) pandemic and economic crisis, Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The Act

was signed into law on March 27, 2020 and includes the Paycheck Protection Program (PPP). According to the Small Business Administration (SBA) website, "the Paycheck Protection Program is a loan designed to provide a direct incentive for small businesses to keep their workers on the payroll. SBA will forgive loans if all employees are kept on the payroll for eight weeks and the money is used for payroll, rent, mortgage interest, or utilities." The available funds are meant to help workers by keeping them employed.

7. In addition, the SBA opened its Economic Injury Disaster Loan (EIDL) program to small businesses as a result of COVID-19. The SBA website explains that the purpose of the EIDL program is "To meet financial obligations and operating expenses that could have been met had the disaster not occurred."

8. On or about March 17, 2023, TIGTA Special Agent Patrick Latchaw received information that the Pimentel had applied for a PPP loan and EIDL for SSI Enterprises, LLC.

Pimentel Loan Applications

Entity	Date Approved	Loan Amount	Loan Type
SSI Enterprises, LLC (EIN: 82-4122770)	5/1/2020	$20,800	PPP Loan
SSI Enterprises, LLC (EIN: 26-2984122)	6/19/2020	$150,000	EIDL

Both applications were approved for a total of $170,800 in CARES Act funds. An additional $2,000 EIDL advance was also awarded to SSI Enterprises, LLC. Law enforcement believes that Pimentel obtained the funds through fraudulent means.

PPP Loan Application

9. On or about April 23, 2020, Pimentel applied for a PPP loan through Citizens Bank for SSI Enterprises, LLC. This loan for $20,800 was approved on May 1, 2020.

10. The email address he provided on the application was kidcash@hotmail.com.

11. IRS Revenue Officer Jennifer Green reviewed the approved PPP loan file as part of an ongoing tax collection case. Green referred the case for potential criminal prosecution after finding indicators of fraud.

12. First, as part of the PPP loan application, Pimentel submitted a 2019 IRS Form 1040 Schedule C that Green confirmed had not been filed with the IRS. This document claimed that Pimentel, through SSI Enterprises, had approximately $3.5 million in gross receipts or sales in 2019 and gross income of approximately $930,000 that year.

13. Second, to qualify for the PPP loan, Pimentel was required to certify on the application that "the Applicant was in operation on February 15, 2020" and "had employees for whom it paid salaries and payroll taxes, or paid independent contractors, as reported on IRS Form(s) 1099-MISCELLANEOUS ("Form 1099-MISC")." A Form 1099-MISC is filed for each person to whom you have paid during the relevant tax year. Employers use Form 941 to report income taxes, Social Security tax, or Medicare tax withheld from employee paychecks. Green confirmed that Pimentel has never filed a Form 1099-MISC or Form 941 for SSI Enterprises, LLC.

14. Similarly, on the loan application, Pimentel stated that he has 10-50 employees despite having never filed an IRS Form 1099-MISC or Form 941 for SSI Enterprises, LLC.

15. Third, Pimentel has two Employer Identification Numbers (EINs) for SSI Enterprises, LLC. Pimentel used EIN "82-4122770" created in 2018 for SSI Enterprises, LLC on the PPP loan application. He also listed that EIN on the Schedule C submitted with the

application. However, Pimentel used EIN "26-2984122," which was created in 2008, to submit an EIDL loan application for SSI Enterprises, LLC and to file 2017 and 2018 tax returns for SSI Enterprises, LLC with the IRS.

16. Fourth, it does not appear that the $20,800 PPP loan proceeds were ever used for any business purposes. Pimentel opened a new business account (ending -8203) and personal bank account (ending -1387) at Citizens Bank on April 21, 2020. Pimentel submitted the PPP loan application on April 23, 2020. The PPP loan proceeds were deposited into the -8203 account on May 4, 2020. Pimentel then wrote checks to himself for $2,600 eight separate times from May 8, 2020 to June 26, 2020, with the memo "PPP Self Employment Payment." On May 18, 2020, Pimentel also wired $10,000 from the -8203 business account to his -1387 personal bank account. The following day, Pimentel wired $15,000 from his personal account to Gemini Trust, a cryptocurrency company.

EIDL Loan Application

17. On or about June 16, 2020, Pimentel applied for an EIDL for SSI Enterprises, LLC. He again provided the contact email address of kidcash@hotmail.com. This loan for $150,000 was approved on June 19, 2020. In addition the SBA awarded a $2,000 EIDL advance.

18. On the EIDL application, Pimentel indicated that SSI Enterprises, LLC has 2 employees. However, as mentioned earlier Pimentel has never filed an IRS Form 1099-MISC or Form 941 for SSI Enterprises, LLC. Moreover, in the earlier PPP application Pimentel claimed SSI Enterprises, LLC had 10-50 employees.

19. Pimentel also claimed SSI Enterprises had gross revenues of $6,790,624 in the year preceding January 31, 2020, and that the cost of goods sold in that same period was

$5,424,959, despite not having even opened his business bank account ending -8203 until April 2020.

20. On June 22, 2020, the EIDL proceeds of $149,900 were deposited into the business account ending -8203. The EIDL advance of $2,000 was deposited into that same account on June 30, 2020.

21. Pimentel certified that he would not misapply the proceeds of the loan on the EIDL application. However, it appears he misused the EIDL funds.

22. On June 29, 2020, Pimentel sent a wire transfer to Argeny Vargas, 37 Knox Street Lawrence, Massachusetts 01841 in the amount of $75,000 from the -8203 business account. Furthermore, Pimentel transferred $20,000 to his -1387 personal account on July 10, 2020. On July 13, 2020, Pimentel made a payment of $48,623.29 from his -1387 personal account to American Express. Pimentel also withdrew $8,000 cash from the -8203 business account on July 14, 2020. On July 17, 2020, Pimentel transferred $47,000 more from the -8203 business account to his -1387 personal account. On July 20, 2020, Pimentel made a $10,000 cash withdrawal from the -1387 account and transferred $15,000 back to the -8203 account. On July 20, 2020, Pimentel made two separate cash withdrawals for $5,000 and $9,000 from the -8203 business account. Finally, on July 27, 2020, Pimentel transferred $20,000 from the -8203 business account to the -1387 personal account. On both July 28, 2020 and July 31, 2020, Pimentel made $10,000 PayPal transfers from the -1387 account to someone with the username Vimal1118.

23. In August 2020, Pimentel was stopped at the Los Angeles International Airport carrying $143,045 in cash. He claimed that he was going to Las Vegas to gamble with the funds. The Drug Enforcement Administration suspected Pimentel was a drug-money launderer and seized the funds.

24. Pimentel listed the e-mail account kidcash@hotmail.com as a form of communication with Citizen's Bank and SBA for the submitted PPP and EIDL loans. The SBA documented multiple attempts to communicate with Pimentel via e-mail after the EIDL loan had been approved and processed, requesting additional insurance and certificate documentation.

25. A subpoena was previously issued to Microsoft requesting certain subscriber information for kidcash@hotmail.com. The subpoena response confirmed that Sully Pimentel is the registered subscriber for that email.

26. A preservation request was sent on November 2, 2023. In general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time.

27. For the reasons set forth above, there is probable cause to believe that the email kidcash@hotmail.com contains evidence, fruits, and/or instrumentalities of the Subject Offenses. In particular, the contents of that email will show whether Pimentel had an actual ticketing business as he claimed on the CARES Act loan applications.

BACKGROUND CONCERNING EMAIL

28. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("email") access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name HOTMAIL.COM, like the email account listed in Attachment A. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic

communications (including retrieved and unretrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. A Microsoft subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

30. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

31. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records

of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

32. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email

communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

34. Based on the forgoing, I request that the Court issue the proposed search warrant.

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

36. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

/s/ Patrick Latchaw
Patrick Latchaw
Special Agent
TIGTA

Subscribed and sworn to me, telephonically, on January 12, 2024

Hon. Andrea K. Johnstone
U.S. Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with kidcash@hotmail.com that is stored at premises owned, maintained, controlled, or operated by Microsoft, a company headquartered at 1 Microsoft Way, Redmond, Washington 98052.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 2, 2023, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from 01/01/2018 to 01/01/2021, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. § 1014 (False Statement to a Bank), those violations involving Sully Pimentel and occurring after January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Evidence that Pimentel used the email account to fraudulently submit loan applications;

(b) Evidence that Pimentel used the email account for SSI Enterprises to conduct a legitimate ticketing business;

(c) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(d) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(f) The identity of the person(s) who communicated with the user ID about the fraudulent loan applications, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Microsoft, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Microsoft. The attached records consist of _____ documents. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Microsoft, and they were made by Microsoft as a regular practice; and

b. such records were generated by Microsoft's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Microsoft in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Microsoft, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature